

Applicant : Oliver Goldman
Serial No. : 10/656,593
Filed : September 4, 2003
Page : 12 of 24

Attorney's Docket No.: 07844-596001 / P549

REMARKS

Claims 1-48 were pending as of the action mailed on April 5, 2006. Claims 1, 20, 26, and 43 are being amended. No new matter has been added. Reexamination and reconsideration of the action are requested in light of the foregoing amendments and the following remarks.

Section 102 Rejections

Claims 1-4, 18, 20, 26-29 and 43 are rejected as allegedly anticipated by U.S. Patent Application Publication US 2005/0021474 ("Geist").

Claim 1. In rejecting claim 1, the examiner stated:

Geist et al. fully disclose a computer implemented method, comprising:
accessing an electronic document using a user application, the electronic document including a digital signature module (Page 10: 0140-0142);

The passage cited by the examiner describes a bar code printed on the face of a check. Geist, ¶¶ 0140-0142. This does not meet the limitations of the claim. The claim recites "an electronic document". A check on which a bar code can be printed is a paper document, not an electronic document. For at least this reason, the rejection of claim 1 should be withdrawn.

The entirety of the cited passage the examiner relies on reads as follows.

[0140] All such critical document data is preferably stored in a PDF 417 two-dimensional bar code 60 printed on the face of the check, to the left of the signature line, just above the MICR [magnetic ink character recognition] code line 90 and the MICR clear band, which is a 0.625-inch high horizontal band located above the lower edge of the check (FIG. 5). The width of the two dimensional bar code on personal checks is preferably approximately three inches, and on commercial checks it may be as long as five inches. The height of the bar code is based on the bar code element size and the number of data bytes contained within, though it will be understood that the dimensions and location of the bar code are not so limited. Other data may be stored in this bar code 60 as well. As known to those skilled in the art, many software tool kits are available for creating PDF 417 bar codes from given ASCII or binary data. Software toolkits are also available to assist in developing bar code reading applications using black and white or gray scale document images.

Applicant : Oliver Goldman
Serial No. : 10/656,593
Filed : September 4, 2003
Page : 13 of 24

Attorney's Docket No.: 07844-596001 / P549

[0141] PDF 417 bar codes are composed of rows of element blocks. Each row is composed of columns of modules, each 17-element-blocks wide. An element block, which is 0.013 inches wide and 0.018 inches tall, produces a bar code that is easily read from standard 200 or 240 dot per inch gray-scale images. Importantly, many check sorters on the market today are capable of imaging a check bar code at this quality level. The bar code element size can be adjusted to facilitate reading printed bar codes from black and white images (as opposed to gray-scale) and/or from images that are of lower or higher resolution. PDF 417 bar codes readable from 200 or 240 dot per inch gray-scale images can store approximately 200 data bytes per square inch of bar code area.

[0142] It will be appreciated to those skilled in the art that other means of storing machine-readable information on the document can be utilized as an alternative to PDF 417 such as Data Matrix, MaxiCode, Astec, or Data Glyphs. All such methods of storing machine-readable information, and similar methods, are intended to be within the spirit and scope of the present invention.

This passage also does not disclose "accessing an electronic document using a user application," as recited in claim 1. Instead, it discloses "storing machine-readable information on the document," which is necessarily a paper document in this context.

Nor does the passage cited by the examiner disclose an electronic document that includes "a digital signature module," as also recited in claim 1. Without changing the scope of the claim, claim 1 has been amended to include a definition of "digital signature module", and so recites that the digital signal module is "operable to perform digital signature operations on the electronic document." Thus, as is clear from the applicant's specification, the digital signature module is executable code that can be executed on a server, for example, and not merely passive data. For at least these reasons, the rejection of claim 1 should be withdrawn.

In rejecting claim 1, the examiner further stated:

Geist et al. fully disclose a computer implemented method, comprising:

....
using the digital signature module to perform one or more digital signature operations on the electronic document in the user application (Page 8: 0119-0121).

Applicant : Oliver Goldman
Serial No. : 10/656,593
Filed : September 4, 2003
Page : 14 of 24

Attorney's Docket No.: 07844-596001 / P549

The passage cited by the examiner describes a trusted third party certificate authority that produces a key pair and signs a certificate. Geist, ¶¶ 0119-0121. The entirety of the cited passage reads as follows.

[0119] a. Certificate Authority 46

[0120] In the preferred embodiments of this invention, a single third party trusted by all participants in the authentication system of the present invention preferably serves as the certificate authority (CA) 46; i.e., the party that issues all the ECDSA certificates described in more detail below. In the simplest and preferred embodiment of the authentication system of present invention, the CA 46 will produce a key pair and sign certificates all in the context of an elliptic curve group defined for all users of the systems. That is, a single elliptic curve group defines the digital signature operation for all participants, including the CA 46. (The CA 46 could produce a separate set of shared parameters to define a different elliptic curve group for issuing digital signatures appearing in public key certificates. Utilizing a different elliptic curve group in issuing public key certificates results in the higher mathematical strength of such digital signatures as compared with those digital signatures used to secure individual bar code strings. This might be useful, for example, in those instances where it is desired that the public key certificate have a longer period of validity than the digital signature for the bar code string on a personal check (which, might have a validity period of only one year, for example). This extra set of elliptic curve parameters could be circulated to all participants, embedded in software, or otherwise provided as loadable data. This data could be authenticated by the participants in some manner at the time of the parameters' retrieval and use.)

[0121] Using the set of common shared parameters 41 which define the basic elliptic curve operations, the CA 46 generates a public/private key pair. The private key portion of the pair issues all digital signatures inside the public key certificate, and is kept under strict control by CA 46. Only the CA 46 can issue valid certificates since the private key required for public key certificate signature is held exclusively by the CA 46. The CA's public key validates all public key certificate signatures and is distributed with all shared parameters to all participants involved

As is clear from reading this passage, it does not in fact describe "using the digital signature module to perform one or more digital signature operations on the electronic document in the user application," which is what claim 1 actually recites.

Applicant : Oliver Goldman
Serial No. : 10/656,593
Filed : September 4, 2003
Page : 15 of 24

Attorney's Docket No.: 07844-596001 / P549

For each of the foregoing reasons, the rejection of claim 1 should be withdrawn.

Claim 18. In rejecting claim 18, the examiner stated:

Geist et al. fully disclose a electronic document, comprising:

....
a digital signature module, the digital signature module being operable upon loading to perform digital signature operations on the electronic content (Page 8: 0119-0121).

The passage cited by the examiner describes a trusted third party certificate authority that produces a key pair and signs a certificate. Geist, ¶¶ 0119-0121. The entirety of the cited passage was just quoted.

As is clear from reading this passage, it does not in fact disclose "a digital signature module" that is "operable upon loading to perform digital signature operations" on electronic content, where both the content and the module are included in the same electronic document. This is what claim 18 actually recites. While Geist may disclose digital signatures upon which signature operations are performed, this is different from actually being able to perform operations, which is what the claim recites.

For each of the foregoing reasons, the rejection of claim 18 should be withdrawn.

Claim 20. The examiner rejected claim 20 stating that:

Geist et al. fully disclose a computer implemented method, comprising:
receiving a signed electronic document, the electronic document
including a digital signature module and a digital signature generated by the
digital signature module (Figure 8; Column 3:0045; Page 0136; Figure 9);

Like claim 1, claim 20 was amended to make clear that a digital signature module can perform signature operations: "the digital signal module being operable to perform digital signature operations on the electronic document."

Thus, for the same reasons that apply to claim 1 and claim 18, Geist does not disclose an electronic document that includes both a module and a signature generated by the module, where the module can perform signature operations on the electronic document that includes the module and signature generated by the module.

Applicant : Oliver Goldman
Serial No. : 10/656,593
Filed : September 4, 2003
Page : 16 of 24

Attorney's Docket No.: 07844-596001 / P549

For each of the foregoing reasons, the rejection of claim 20 should be withdrawn.

Claim 26. Claim 26 was rejected simply as a computer claim corresponding to claim 1.

The rejection of claim 26 should be withdrawn, therefore, for the same reasons that apply to claim 1.

Claim 43. Claim 43 was rejected simply as a computer claim corresponding to claim 20.

The rejection of claim 43 should be withdrawn, therefore, for the same reasons that apply to claim 20.

Section 103

Claims 5-14, 23-25, 30-39 and 46-48 were rejected as allegedly unpatentable over Geist in view of U.S. Patent Application Publication US 2003/0023564 ("Padhye").

Claim 5. Claim 5 stands rejected in view of Geist and further in view of Padhye. In rejecting claim 5, the examiner stated:

Geist et al. do not explicitly disclose using the digital signature module includes using the digital signature module running on a server. Padhye et al. in analogous art, however, disclose using the digital signature module includes using the digital signature module running on a server (Page 3: 52C; Figure 10: 740; Column 3: 0037). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Geist et al. to include using the digital signature module includes using the digital signature module running on a server.

The applicant understands the examiner's reference to "Page 3: 52C" to be intended to refer to item 52c in Figure 3. This is described as a digital signature that is included in a license 52. ¶ 0030.

Figure 10 item 740 is a license server. The uses and operations of license server 740 are described in the following paragraphs of Padhye:

[0071] The license server 740 is provided with a public key 744 from the point of capture system 704, and is responsible for issuing both the consumer license 630 and the distribution license 620 from the rights label 750 stored in the license server 740. The rights label 750 includes metadata

Applicant : Oliver Goldman
Serial No. : 10/656,593
Filed : September 4, 2003
Page : 17 of 24

Attorney's Docket No.: 07844-596001 / P549

752, distributor rights 625, consumer rights 635, and the distribution key 624 as shown. In a manner similar to that previously described, the distribution key 624 itself is encrypted using the public key 744 from the point of capture system 704. Thus, the distribution key 624 itself, must be decrypted so that the distribution key 624 can be used to decrypt protected content. Further details regarding generation of the distribution key 624 is discussed relative to FIG. 11. Metadata 752 is included in the rights label 750 that may be used for authentication purposes. The distributor rights 625 may include meta-rights such as rights to offer, grant, obtain, transfer, delegate, track, surrender, exchange, and revoke usage rights to/from others. Meta-rights can also include the rights to modify any of the conditions associated with other rights. For example, a meta-right may be the right to extend or reduce the scope of a particular right or the validation period of a right.

[0075] When attempt is made by the end user 612 to purchase protected content, the public key 613 of the end user 612 which was previously obtained through an activation process, is sent to the license server 740. The license server 740 uses the public key 613 to encrypt the distribution key 624 required to decrypt the protected content, and generates the consumer license 630 using components of the rights label 750. In particular, the consumer rights 635 and the distribution key 624 are used to generate the consumer license 630, the consumer license 630 being completed by inclusion of the metadata 754 that may be used for authentication purposes. The license 630 can then be downloaded by the end user 612 and used for accessing the scheduled future event.

[0076] The above described process for obtaining a consumer license 630 by the end user 612 is somewhat similar to conventional DRM systems. However, in contrast to conventional DRM systems, the obtained consumer license 630 cannot be used for any present content, but instead, serves as a "ticket" for a future event which may be a live event. The consumer license 630 is generated in accordance with the consumer rights 635 that have been specified to the end user 612. Thus, in the manner described above, the license server 740 of the preferred embodiment makes a distinction between the rights specified for the distributor and the rights specified for the consumer to generate a distributor license 620 or a consumer license 630 accordingly.

[0077] FIG. 11 is a schematic illustration showing the generation of the distribution key 624 that is a component of the rights label 750 in accordance with one embodiment of the present invention. The distribution key 624 is required for generating the distribution license 620 and the

Applicant : Oliver Goldman
Serial No. : 10/656,593
Filed : September 4, 2003
Page : 18 of 24

Attorney's Docket No.: 07844-596001 / P549

consumer license 630 which are necessary for distributing and allowing use of protected content that is to occur in the future, such as a future event. Through a software application, the content distributor 702 initially creates the distribution key 624, which is a symmetric encryption key. The distribution key 624 is protected from tampering by encrypting it with the license server's 740 public key 742 so that only the license server 740 will be able to decrypt the distribution key 624. In this regard, the distribution key 624 is preferably stored in the license server 740 in order to provide better security and to track its use.

[0078] Moreover, as previously noted, additional metadata 752 is created and stored in the rights label 750. This metadata 752 is later inserted into the header information of the video stream that is generated by the point of capture system 704 during the live event. This metadata 752 may be used by the end users 612 to authenticate the issued licenses. The rights label 750 is transferred and stored in the license server 740 and may also be updated therein. The distribution key 624 is then issued as a component of the distributor license 620 and/or the consumer license 630 to a distributor and/or end user 612, respectively, in the manner described relative to FIGS. 9 and 10. The above described process is somewhat similar to processes used in conventional DRM systems except that the distribution key 624 is not immediately used to protect or use content, but it is saved for later use when the protected content is to be distributed closer to the time of the actual future event.

[0079] The following describes an example workflow that may be used to operate a DRM system in accordance with one embodiment of the present invention as applied to protected distribution and viewing of a future event. Thus, FIGS. 7 to 11 and various components identified therein should be referenced to facilitate understanding of the workflow. Initially, the content distributor 702 decides to offer a future event for sale, for instance, a future sporting event. The content distributor 702 creates the distribution key 624 which is a symmetric encryption key. The distribution key 624, together with additional information including distributor rights 625 and metadata 752 is encoded in rights label 750. The rights label 750 is then transferred to the license server 740 at which the consumer rights 635 is also added to the rights label 750.

[0080] The vendor 730 which may be a storefront or a web site, offers for sale the right to view the future event. End user(s) 612 desiring to use or otherwise view the future event, accesses the vendor 730 via the Internet 610 to purchase, or otherwise obtain, the right to view the future event. During the purchasing transaction, the vendor 730 interacts with the license

Applicant : Oliver Goldman
Serial No. : 10/656,593
Filed : September 4, 2003
Page : 19 of 24

Attorney's Docket No.: 07844-596001 / P549

server 740 to generate the consumer license 630 in the manner described above relative to FIG. 10 from rights label 750 so that the end user 612 can download the consumer license 630 to the user's 612 rendering device 626 or any other appropriate device such as a computer, hand held device, etc. for future use in viewing the event.

[0081] During this time when the right to view the future event is offered for sale via the vendor 730, but prior to the start of the actual event, the content distributor 702 requests for the distributor license 620, which is issued by the license server 740 in the manner described above relative to FIG. 9. The distributor license 620 is then used by the point of capture system 704 to protect the content while capturing the live performance of the event, for instance, the sporting event 602. The point of capture system 704 processes the video data from the capturing device 604 on-the-fly, and transmits now protected content 605 to the streaming server 616.

Finally, paragraph 0037, cited by the examiner, reads as follows:

[0037] DRM system 10 addresses security aspects of protected content 42. In particular, DRM system 10 may authenticate license 52 that has been issued by license server 50. One way to accomplish such authentication is for application 60 to determine if licenses 52 can be trusted. In other words, application 60 has the capability to verify and validate the cryptographic signature, or other identifying characteristic, of license 52. Of course, the example above is merely one way to effect a DRM system. For example, license 52 and protected content 42 can be distributed from different entities. Clearinghouse 90 can be used to process payment transactions and verify payment prior to issuing a license. Whereas DRM system 10 effectively addresses security aspects of protected content 42, the system is operable only when protected content 42 is in existence. DRM system 10 cannot readily provide protection to content that is not yet in existence, such as a video stream for a future event.

The passages cited by the examiner describe how a DRM (Digital Rights Management) system may authenticate a license that has been issued by a license server. Padhye, ¶ 0037 This does not meet the limitations of the claim. The claim recites that "using the digital signature module includes using the digital signature module running on a server." There is nothing in the cited portion of Padhye that describes a digital signature module – or anything else that is "operable to perform digital signature operations on the electronic document" – that runs on a

Applicant : Oliver Goldman
Serial No. : 10/656,593
Filed : September 4, 2003
Page : 20 of 24

Attorney's Docket No.: 07844-596001 / P549

server. Note that claim 5 recites accessing an electronic document that includes a module that can perform signature operations on the document, using that module running on a server to perform at least one such signature operation on the electronic document itself. The applicant submits that this combination of features is not found separately or in combination in Geist and Padhye.

For at least this reason, the rejection of claim 5 should be withdrawn.

In rejecting claim 5, the examiner further stated:

This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so to provide a point of capture system adapted to generate content, the right information having secure mechanism that secures when the content when the content is generated as suggested by Padhye et al. (Page 2: 0013).

This statement provides no factual basis supporting the rejection. All of the features mentioned by the examiner are already found in Padhye, so the purported motivation provides no reason to combine Padhye with anything other teaching. In rejecting claims as obvious, it is incumbent upon the examiner to establish a factual basis to support the legal conclusion of obviousness. *See In re Fine*, 837 F.2d 1071, 1073, 5 USPQ2d 1596, 1598 (Fed. Cir. 1988).

The passage cited by the examiner reads in its entirety as follows.

[0013] A first aspect of the invention is a rights management system for managing use of content having usage rights associated therewith. The system comprises a point of capture system adapted to generate content of a future event when the event occurs. The system also comprises a content distributor adapted to generate a rights label having usage rights associated with content of the future event before the content is generated by the point of capture system, the rights label having a securing mechanism that secures the content when the content is generated. The system further comprises a license server adapted to store the rights label and to issue a license associated with the content from the rights label before the content is generated, the license including a mechanism for unlocking the securing mechanism, and where the content distributor is further adapted to distribute the license before the content is generated.

Applicant : Oliver Goldman
Serial No. : 10/656,593
Filed : September 4, 2003
Page : 21 of 24

Attorney's Docket No.: 07844-596001 / P549

A person having ordinary skill in the art would have no motivation to combine Geist and Padhye because Geist describes a system for authentication of individual paper documents that have already been created, such as personal checks and commercial checks, Geist, ¶ 0007, whereas Padhye describes a method for licensing use of digital content that has not been created yet, Padhye, ¶ 0012.

For the foregoing reasons, the rejection of claim 5 should be withdrawn.

Claims 15, 16, 21, 40, 41 and 44 were rejected as allegedly unpatentable over Geist et al. in view of U.S. Patent No. 6,796,489 ("Slater et al.").

Claim 15. In rejecting claim 15, the examiner stated:

Geist et al. discloses a computer implemented method, comprising:
embedding a digital signature module in an electronic document, the
digital signature module being operable to perform one or more digital
signature operations on the electronic document (Figure 8; Figure 9)

Figure 8 describes a "check reading system". Figure 9 is a flowchart describing a process that begins with retrieving a bar code from a check and verifies the check using a PIN or other confirming information. While the bar code may include a digital signature, it does not include a digital signature module that can "perform one or more digital signature operations on the electronic document" as recited in the claim.

The examiner then acknowledges that "Geist et al. do not explicitly disclose embedding a digital signature module in an electronic document." The examiner finds this feature in Slater at Figure 3A-3E and page 10, lines 1-41 (the applicant assumes the examiner is referring to column 10 of the patent). The paragraphs to which the examiner refers (which begin on line 64 of column 9) read in their entirety as follows:

FIGS. 3A, 3B, 3C, 3D, and 3E are block diagrams that illustrate how an electronic document can be both reconstructed, verified, and/or validated. FIGS. 3A through 3E represent different states of the same electronic document, each of which can be reconstructed. FIG. 3A represents a recorded electronic document 300 after the electronic document has been verified and validated. FIG. 3B represents the electronic document 310

Applicant : Oliver Goldman
Serial No. : 10/656,593
Filed : September 4, 2003
Page : 22 of 24

Attorney's Docket No.: 07844-596001 / P549

before it is recorded and the electronic document 310 has not been digitally signed by the recorder. FIG. 3B also represents a reconstructed document that is used to validate the digital signature of the recorder.

FIG. 3C represents the electronic document 320 before it is digitally signed by the notary public and the electronic document 320 does not have a digital notary signature. FIG. 3C also represents a reconstructed electronic document for verifying the digital signature of the notary. FIG. 3D represents an electronic document 330 that has only been signed by the signer A and does not have the digital signature B 331 of signer B. Finally, FIG. 3E represents the electronic document 340 before it is digitally signed by the signer A.

In FIG. 3D, the signature A 302 is embedded. In FIG. 3C, the signature A 302 and the signature B 303 are embedded. In FIG. 3B, the notary signature 304 is embedded in addition to the signature A 302 and the signature B 303. In FIG. 3A all necessary signatures, including the recorder signature 305, are embedded in the electronic document 300.

FIGS. 3A through 3E thus illustrate an electronic document that has been signed in stages. The first or unsigned stage or state of the electronic document is represented by FIG. 3E and the final or fully signed state or stage of the document is represented by FIG. 3A. Any of the document stages represented by FIGS. 3A through 3E can be reconstructed from a later stage. For example, the electronic document 330 of FIG. 3D can be reconstructed from the electronic document 320 of FIG. 3C.

Reconstructing an electronic document ensures that the electronic document has not been changed or altered and is also used when a digital signature is validated. For example, if a first signer digitally signs a document and emails that document to a second signer, the second signer desires some assurance that they are executing the same document executed by the first signer. This can be accomplished by reconstructing the electronic document to its previous state in this example.

These paragraphs describe the figures to which the examiner also referred.

It is clear from reviewing the quoted paragraphs that while Slater does disclose embedding a digital signature in an electronic document, Slater does not disclose embedding a digital signature module, which is what claim 15 actually recites. The module is recited as being operable to perform one or more digital signature operations on the electronic document. A

Applicant : Oliver Goldman
Serial No. : 10/656,593
Filed : September 4, 2003
Page : 23 of 24

Attorney's Docket No.: 07844-596001 / P549

digital signature is not the kind of thing that can perform operations. Slater, for example, describes digital signatures as follows:

When a digital signature is employed to sign a document, the signer first identifies exactly what is being signed. The document or data identified by the signer is hashed to generate a hash result that is essentially unique to the document. Then, the hash result is converted into a digital signature using a private key of the signer to encrypt the hash result. In this manner, both the document and the private key are related to the digital signature. [Col. 1 lines 46-53]

Thus, Slater does not in fact disclose the feature that the examiner acknowledges is lacking in Geist.

For at least this reason, the rejection of claim 15 should be withdrawn.

Claim 40. Claim 40 was rejected simply as a computer claim corresponding to claim 15.

The rejection of claim 40 should be withdrawn, therefore, for the same reasons that apply to claim 15.

Conclusion

All of the rejections of the pending independent claims have been addressed. The rejections of the dependent claims should be withdrawn for at least all the reasons that apply to their respective independent base claims.

For the foregoing reasons, the applicant submits that all the claims are in condition for allowance.

By responding in the foregoing remarks only to particular positions taken by the examiner, the applicant does not acquiesce with other positions that have not been explicitly addressed. In addition, the applicant's arguments for the patentability of a claim should not be understood as implying that no other reasons for the patentability of that claim exist.

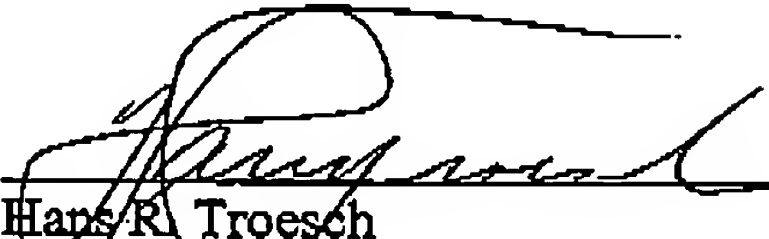
Applicant : Oliver Goldman
Serial No. : 10/656,593
Filed : September 4, 2003
Page : 24 of 24

Attorney's Docket No.: 07844-596001 / P549

Please apply any charges or credits to deposit account 06-1050.

Respectfully submitted,

Date: 05 Jul 06


Hans R. Troesch
Reg. No. 36,950

Customer No.: 021876
Fish & Richardson P.C.
Telephone: (650) 839-5070
Facsimile: (650) 839-5071

50344532.doc